



## King's Research Portal

DOI:

[10.1177/1368431016667623](https://doi.org/10.1177/1368431016667623)

*Document Version*

Peer reviewed version

[Link to publication record in King's Research Portal](#)

*Citation for published version (APA):*

Aradau, C., & Blanke, T. (2017). Politics of prediction: security and the time/space of governmentality in the age of big data. *European Journal Of Social Theory*, 20(3), 373-391. <https://doi.org/10.1177/1368431016667623>

### **Citing this paper**

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

### **General rights**

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

### **Take down policy**

If you believe that this document breaches copyright please contact [librarypure@kcl.ac.uk](mailto:librarypure@kcl.ac.uk) providing details, and we will remove access to the work immediately and investigate your claim.

# **Politics of prediction: Security and the time/space of governmentality in the age of big data**

## **Abstract**

From ‘connecting the dots’ and finding ‘the needle in the haystack’ to predictive policing and data mining for counterinsurgency, security professionals have increasingly adopted the language and methods of computing for the purposes of prediction. Digital devices and big data appear to offer answers to a wide array of problems of (in)security by promising insights into unknown futures. This paper investigates the transformation of prediction today by placing it within governmental apparatuses of discipline, biopower and big data. Unlike disciplinary and biopolitical governmentality, we argue that prediction with big data is underpinned by the production of a different time/space of ‘between-ness’. The digital mode of prediction with big data reconfigures how we are governed today, which we illustrate through an analysis of how predictive policing actualises between-ness as hotspots and near-real-time decisions.

**Keywords:** governmentality, prediction, big data, time/space, security, policing

## **Introduction**

‘Big-data technology is the digital-age equivalent of the telescope or the microscope’ (Lohr 2015, 9). In recent years, big data has promised to revolutionise digital capabilities and practices of governance. In the world of security professionals, the emergence of ‘big data’ has become linked to the promise of prediction and proactivity for ‘connecting the dots’ and ‘finding the needle in the haystack’. As security professionals have increasingly adopted the language and methods of computing for the purposes of prediction, they have taken inspiration from other big data applications in the corporate world. The Snowden revelations have shown how intelligence agencies deploy similar technologies as commercial big data companies, and how they have increasingly mobilised these technologies to find unknown patterns and relations (National Security Agency 2008, GCHQ 2011). Yet, big data is not only used by businesses and intelligence agencies, but increasingly by the police, border guards, and even humanitarian actors (Akhgar et al. 2015, Cheng et al. 2016, Meier 2015). Intelligence, counter-terrorism, policing and cybersecurity have been transformed by the promise of big data and predictive analytics to uncover unexpected patterns and pinpoint potentially suspect ‘needles’.

Incorporating massive, dynamic, and heterogeneous datasets which can be increasingly stored and processed, big data-based predictive analytics appears to harbour new capacities of peering into the future and revealing the unknowns to be tamed and governed (Kitchin 2014, boyd and Crawford 2012, Cukier and Mayer-Schoenberger 2013, Lyon 2014, Aradau and Blanke 2015). For security professionals, predictive analytics with big data holds the promise to secure the

future by anticipating the ‘next terrorist attack’ and apprehending potential criminals before they can strike. Therefore, predictive analysis is harnessed for the purposes of anticipatory governance to address an increasing array of security issues, from crime to terrorism, and from poverty to natural disasters.

Neither prediction nor anticipation is a new phenomenon.<sup>1</sup> From fortune telling to statistical prognosis and from futurology to big data, prediction has long informed the rationalities of human action and practices of governing. As François Ewald (2012, 47) has noted, the predictive function is today, just as yesterday, inscribed within the apparatuses of government. Prediction has thus long been central to governmental interventions and has been shaped, in turn, by different regimes of power/knowledge. For Reinhardt Koselleck, the incorporation of prediction within governmental action was inaugurated by the French Revolution, which rendered the future ‘so obscure that its recognition and mastery have become the constant task of politics’ (2004, 72). Independent of how temporal boundaries are drawn for the governmentalisation of prediction, these historical reflections locate different modes of prediction in regimes of power/knowledge. Thus, rather than a shift from the predictable to the unpredictable, as diagnosed by Ulrich Beck (2009), from regimes of truth to regimes of anticipation (Adams, Murphy, and Clarke 2009), from topological to temporal governance (Rouvroy 2010), or from risk to new techniques of governing uncertainty (O'Malley 2004, Aradau and van Munster 2011, Samimian-Darash and Rabinow 2015), prediction has not vanished today. Big data has revitalised the promise of prediction across social, political and economic worlds.

This paper develops a ‘history of the present’ of prediction by asking: what difference does big data make for how we are governed today? We attend to what Michel Foucault has called the ‘inflection of the curve’ (Foucault 1978) and explore the reconfiguration of prediction within governmental regimes of power/knowledge. As big data promises to ‘unlock’ the blockages and limitations of disciplinary and biopolitical techniques of government, we argue that a digital mode of prediction emerges today through the reconfiguration of time/space through calculations of ‘between-ness’. We coin the notion of ‘between-ness’ to capture the logic of predictive analytics.

To develop this argument, the paper proceeds in three stages. We firstly revisit Foucault’s analyses of governmentality to show how prediction has been differentially incorporated within apparatuses of discipline and biopower. Secondly, we explore the production of prediction within a regime of governing through big data by attending to the techniques of predictive analytics. Thirdly, we illustrate the materialisation of predictive analytics with big data in security practices through controversial developments in predictive policing. In conclusion, we develop a series of remarks on the social and political implications of prediction in a regime of ‘between-ness’.

## **Governmentalising prediction: discipline, biopolitics, big data**

‘We live in a predictive society’ (Davenport 2014b).

Prediction as *pre-dictum*, saying in advance or foretelling evinces an orientation towards the future. This turn to the future has taken different forms historically and has been shaped by particular regimes of power/knowledge. From divination to prognosis and from trends to forecasts, different modes of prediction have gained and lost epistemic and social credibility. Histories of the future have traced this struggle for knowledge from the rise and wane of prognosis and astrology, through to the scientification of the future through risk and then futurology in the 20<sup>th</sup> century (Minois 1996, Koselleck 2004). Prediction, alongside forecasting and project is one of 'contemporary industrial societies' ways of telling the future' (Adam and Groves 2007).

More recently, debates about digital technologies and digital data have also drawn attention to the renewed promise of prediction. Adrian Mackenzie has analysed the production of prediction through the computational techniques of machine learning, which have been used for at least half a century, and has argued that 'machine learning literature has principally retold a kind of romance, in which, after many trials and tribulations with unruly, messy, mixed or 'dirty' data, epistemic order and predictive power prevail over error and the unexpected' (Mackenzie 2015, 436). This romance that machine learning has promoted is reiterated in recent discourses of predictive analytics with big data. According to Steve Lohr, the technology reporter of the *New York Times*, 'seeing into the future' is one of the main promises attached to big data (Lohr 2015). For computer scientists assessing the transformations that big data entails, 'prediction is the hallmark of Big Data' (Ekbja et al. 2015). Big data promises the detection of previously unknown patterns and the discovery of surprising hidden knowledge that holds the key to preventing future crimes or terrorist attacks.

Thus, the predictive promise of big data intersects with security professionals' search for new capabilities to pre-empt the 'next terrorist attack', migration crisis, insurgency or crime. If intelligence professionals have long been interested in the prediction of actions inferred from the identity of suspect enemies, digital data and analytics have increasingly focused on predicting what might happen (Adey 2009). Big data thus promises a 'revolution' for security practices, from counter-terrorism and border control to policing crime and emergency responses. It does so by challenging the over-reliance on frequencies of past events and their projection of onto the future (Amoore 2014, Aradau and van Munster 2011, Hansen 2015, Massumi 2009). The move from (past) data to future prediction is a key claim of analytics with big data. Big data thus leads to a 'reinforced future-orientation', which is 'likely to exacerbate the severance of surveillance from history and memory and the assiduous quest for pattern-discovery will justify unprecedented access to data' (Lyon 2014, 6).

Connecting the dots has become insufficient for security professionals who now formulate the predictive promise of big data as 'finding the needle in the haystack' (Aradau 2015). What mode of prediction emerges at the intersection of big data and security today? To understand the difference that prediction makes for governing practices today, we start by placing prediction within Foucault's analyses

of discipline and biopower. Although Foucault did not speak of prediction when analysing governmentality, we take Ewald's point seriously that we need to reinsert prediction within governmental apparatuses to understand the predictive rationality of big data in order to analyse the specific inflection of prediction in governmental practices today.

Rather than opposing modes of 'scientific prediction' to pre-scientific or non-scientific modes of future-telling (Adam and Groves 2007), re-reading Foucault's analyses of discipline and biopower can show how different modes of prediction emerge in regimes of power/knowledge. Given the association between prediction and the future, scholars drawing on Foucault's work have located prediction within biopolitical apparatuses and the actuarial turn in governance (Harcourt 2008). Statistical techniques and insurance practices focus on the occurrence of events: 'what had been exceptional events that disrupted the normal order become predictable occurrences' (Lakoff 2007, 250). Biopolitical techniques tame contingency, while disciplinary mechanisms are deployed in the enclosed spaces of the prison, factory or military barracks.<sup>2</sup> This apparent disjunction of time and space in Foucault's analytics of disciplinary and biopolitical apparatuses has simultaneously dis-associated prediction from discipline. The temporality of biopolitics, with its focus on managing populations by calculating the frequency of events and taming their contingency, is thus the temporality of prediction par excellence: an orientation towards the aleatory future, whose contingency can be 'tamed' through statistical knowledge.

Yet, this reading of prediction misses two important aspects of Foucault's notion of governmentality. The first one is what could be seen as a generally predictive orientation of governmentality. Understood as the 'conduct of conduct' or 'a form of activity aiming to shape, guide or affect the conduct of some person or persons' (Gordon 1991, Dean 1999), governmentality entails some form of predictive calculability about action and its effects. The techniques of governmentality are techniques of prediction inasmuch as they problematize and aim to shape the 'not-yet' of action. The second element in our analysis of prediction is the co-constitution of time/space in governmental practices. In our approach, prediction is not exclusively about the future, but about the configuration of time/space in governmental apparatuses. To recast prediction as a technique of power/knowledge within governmental apparatuses, we revisit the often-rehearsed narrative of transformation from the disciplinary space of the Panopticon to the biopolitical taming of aleatory events.<sup>3</sup>

Reading discipline and biopolitics as co-constitutive of time/space allows us to trace the governmentalisation of prediction and the transformations big data entails today. Although a disjunction of space and time appears in Foucault's own remarks, such as in his opposition of the 19<sup>th</sup> and 20<sup>th</sup> century as epochs of history and space respectively, Foucault has cautioned that 'it is not possible to disregard the fatal intersection of time and space' (Foucault 1986, 22). His analyses of space – from heterotopia and territory to the architecture of the prison and the milieu of biopolitical interventions – are effectively conjoined with the historical constitution of time. For Foucault, time/space is co-constituted through mechanisms of power/knowledge and

in that sense it is entangled with different modes of prediction.

How does prediction emerge within disciplinary and biopolitical government? The Panopticon as a space that ‘concentrates, focuses and encloses’, where the mechanisms of its power will function fully and without limit’ (Foucault 2007, 67) is co-constituted through time. Discipline does only arrange bodies in space, but must be understood through mechanisms of adding up and capitalising on time. As David Murakami Wood (2007, 260) has noted, what is central to disciplinary apparatuses is ‘the spatial and temporal distribution and regulation of the body’. Time is segmented and separated, so that it becomes exhaustively used: training, eating, exercising, all this is allocated a particular temporal segment within ‘clock’ time. This segmentation of abstract or ‘clock’ time is conjugated to a progressive time, which leads to the final point of the ‘normal’, when disciplinary mechanisms become redundant. ‘The disciplinary methods’, Foucault pointed out, ‘reveal a linear time, whose moments are integrated one upon another, and which is orientated towards a terminal, stable point; in short an “evolutive” time’ (Foucault 1991 [1977], 174). Disciplinary mechanisms display an orientation towards the future, which is the stable point of normality to be reached by acting upon particular spaces. For Foucault (2008, 70), disciplinary power ‘looks forward to the future, towards the moment when it will keep going by itself and only a virtual supervision will be required, when discipline, consequently, will have become habit’.

As the disciplinary linear time needs to be learned, artificial spaces are constructed to delimit the ‘not-yet’ corrected individual from normal individuals. The conduct of subjects is shaped through spatio-temporal techniques of division and separation. In this time/space configuration, prediction is effectively a present *diction*, an art of ‘normation’ where the norm precedes the separation and temporal distinction between what is now is what is the final point of the normal. Prediction is effectively a governmental *projection* of norms upon an artificial, heterotopic time/space.

A different time/space emerges for prediction with biopolitical government. Prediction is not simply the effect of statistical calculations of risk which ‘tame’ contingency and aleatory events (Dillon 2007, Massumi 2009). For Foucault, the time of aleatory events is co-constitutive of the spatiality of the milieu as ‘an ensemble of natural givens – rivers, marshes, hills – and an ensemble of artificial givens- an agglomeration of individuals, house etc.’ (2007, 22-23). Thus, biopolitical mechanisms ‘try to plan a milieu in terms of events or series of events or possible events’ (Bigo 2008, 108).<sup>4</sup> Within the time/space of biopolitics, prediction does not focus on stopping or avoiding an event, but on managing its consequences within a milieu. Unlike the artificial space of the prison, the milieu is about ‘natural givens’ whose positive elements need to be maximized while risks and undesirable elements are minimised (Foucault 2007, 34). Biopolitical prediction relies on a future that ‘is not exactly controllable, nor precisely measured or measurable’ (Foucault 2007, 35). It depends on statistical knowledge about the past so that prediction is effectively *prospective retro-diction*. Or, to put it differently, biopolitics and statistical techniques of measurement capture the mathematisation of prediction (Ewald 2012). The prospective intervention to modulate the potentialities and consequences of events in

a given space is made possible by the retroactive creation of a series of events whose frequencies can be calculated probabilistically.

While Foucault has often emphasised that biopolitics does not replace discipline and sovereignty, he accounts for the emergence of biopolitics through the limitations of disciplinary techniques of government. Discipline was an intensive and costly technique of power, while biopolitics appeared to govern in less insidious and costly ways. Our insertion of prediction with governmental apparatuses adds another dimension to Foucault's analysis of this transformation. Disciplinary mechanisms relied upon the possibility of extending the time-space of the present norm into a controllable future. With the 'avalanche of printed numbers' (Hacking 1982) and the development of statistical methods, prediction could combine controllability and contingency. The future was no longer knowable and controllable through knowledge of the individual, but contingency could be tamed through the creation of series at the level of populations. Uncertainty could be simultaneously recognised, and quantified in terms of probabilistic risk. Yet, these mechanisms to tame uncertainty have once more become insufficient when data is abundant, comes in heterogeneous forms from anywhere, and with increased velocity.

Big data promises to address the limits of biopolitical techniques of governing and statistical methods of knowledge production. Debates about big data problematise exactly the limitations of traditional statistical procedures, which work with particular population groups and samples, longer time intervals and spatial delimitation (often national territories), and do not capture the detailed relationships between individuals and groups as they exist and change in particular situations. In contradistinction to what is now seen as sparse statistical data, big data techniques extend across space and time as data is relentlessly captured and leaked in forms that are 'heterogeneous and unstructured— text, images, video—often emanating from networks with complex relationships between their entities' (Dhar 2013, 64). The traditional model of statistics of particular populations appears insufficient to represent all these relationships and their hidden knowledge of the future. As Ewald points out, big data does not just address the gaps of statistics so that risk management can become more efficient but big data and risk are 'heterogeneous worlds that would not so much be in complementary relationships as in relationships of contestation and substitution' (2011, 81). Big data capitalises on this imaginary of data deluge, unstructured formats and unexpected insights to revitalise the promises of prediction. The next section unpacks the digital mode of prediction enacted through big data.

### **Digital modes of prediction: Predictive analytics with big data**

Predictive analytics as the 'process of discovering interesting and meaningful patterns in data' (Abbott 2014, 3) has been key to security professionals' dream of acceding to the future and interrupting the 'next terrorist attack' before it can become a full-fledged event. Predictive analytics draws on techniques of traditional statistics, but also machine learning, artificial intelligence, and data mining in order to automate 'data-driven algorithms [that] induce models from the data' (Abbott 2014, 3). Thomas

Davenport, who advocates the use of predictive analytics for the business world, locates the birth of analytics in the 1950s business analytics, which relied on structured sources of data that were largely internal to companies (2014a). Compared to the 1950s, predictive analytics now uses data from anywhere. Data is collected both through extraction and capture by digital devices under the mantra of ‘collect it all’ (Crampton 2015). With big data collected from anywhere and in heterogeneous form, predictive analytics has emerged as a distinct practice from the traditional exploration of expectations using statistics. For predictive analytics with big data, the ‘data is king’, while for statistics ‘the model is king’ (Abbott 2014, see also Lohr 2015). Thus, even as data had been widely used for statistics and biopolitical governmentality, data takes on a different meaning with ‘big data’, as it is imagined as a reservoir of unexpected insights which can transform practices of governance. As one of the most mediatized practitioners deploying data mining for security has put it, ‘[b]ig data is not so much about big data as it is about an enhanced ability to extend and more effectively realize the promise of predictive analytics’ (McCue 2015, 380).

To explore the digital mode of prediction that has emerged through the promise of big data to uncover previously unknown patterns in massive data sets, we discuss how the techniques of predictive analysis enact time/space. Similarly to Mackenzie (2015), we use key textbooks and how-to manuals for predictive analytics, alongside reports and publications by practitioners working at the intersection of big data and security.<sup>5</sup> Our selection of textbooks and how-to manuals has focused on the most widely cited practitioners of predictive analytics, on the one hand, and practitioners working at the intersection of big data and security, on the other.<sup>6</sup> By analysing the practitioners’ methods and techniques, our aim is to highlight shared premises and assumptions with which techniques of predictive analytics work. Our methodological contention is that, independent of the specific algorithms developed, prediction requires a series of shared assumptions and techniques. Our aim is to address the limits of proprietary, secret technologies or difficult to understand algorithms in the ‘black box society’ (Pasquale 2015). While the inscrutability of algorithms, which make ‘predictions based solely on algorithm-derived correlations opaque and difficult to interpret’ (Chan and Bennett Moses 2015, 16, see also Pasquale 2015, Introna 2015) is undeniable, our methodological contention is that we can go beyond the details of particular algorithms to understand the shared assumptions and techniques that practitioners learn in order to be able to analyse digital data.<sup>7</sup>

Predictive analytics as presented in the textbooks and practitioners’ guidelines focuses on finding patterns in data from any source by relying on an ‘ontology of association’ (Amoore 2011, 27). In order to be able to process the data as it comes and nevertheless find associative patterns, predictive analytics begins by breaking up captured data into describable and measurable ‘features’ or attributes of interest. Compared with statistical variables, features are different in a number of important ways. Firstly, they can represent anything and anybody and define together a feature space that has as many dimensions as there are features and as many entries as there are data records. Secondly, features can ‘come from almost any form of data (text,



images, video, transactions, sensors), not just the variables measured using classical statistical tabulations of surveys, polls or random sampling' (Mackenzie 2015, 433). Finally, predictive analytics algorithms can develop their own higher-level features by combining existing ones or create completely new ones. They thus learn how to represent data in the feature space.

Therefore, in predictive analytics, data is analysed in abstract spaces, which are a geometrical representation of all the data available for algorithmic processing. In the language of predictive analytics, these abstract spaces become the 'feature space' in which algorithms and practitioners operate. Feature spaces are high-dimensional geometric spaces where 'a notion of "distance" makes sense' (Schutt and O'Neil 2013, 81). Understanding objects depends here on the 'geometry of the space' (Van Rijsbergen 2004, 20) these are captured in. A range of different geometrical measures and distances can be used in predictive analytics (Provost and Fawcett 2013), by which any object can be represented as a dot or data point in this space through a combination of features. In principle, there is no limit to the number of features that can be used to build this artificial space. Feature spaces can have hundreds, thousands or hundreds of thousands of features and dimensions, depending on how much a computer can process. This can lead to a 'combinatorial explosion' of possible feature combinations' (Janert 2010, 425) and what boyd and Crawford have named the apophenia of big data – 'seeing patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions' (boyd and Crawford 2012, 553).

The emergence of relations and connections in feature spaces relies on calculations of 'between-ness'. We use the notion of 'between-ness' to capture the widely-used measure of the shortest path between two data points in the feature space. Between-ness thus measures the connection and relatedness between anything mapped into the feature space. It is not simply a connection or network, but an understanding of similarity and difference based on geometrical distance. The classification algorithms used in predictive analytics rely on assumptions about how the feature space can be optimally partitioned and the calculability of 'between-ness' as a measure of how distant or close data points are. A digital mode of prediction thus emerges in a regime of between-ness.

Predictive analytics algorithms manipulate the feature space and its various combinations in order to create so-called 'labels' for each object that is already assigned by past data in the feature space and predict new labels for all possible objects in the feature space. In order to label everything in the feature space, algorithms work it by dividing it into subspaces through 'dividing lines' or so-called 'decision boundaries' (Janert 2010, 414) that separate some dots in the feature space and bring others together. Thus, predictive analytics entails bringing together and dividing data points by splitting the abstract feature space into distinct areas, as Figures 1 and 2 illustrate. In Figure 1, we show how a 'decision tree' algorithm draws boundaries in a two-dimensional feature space, by combining decisions made over a spatial feature on the horizontal axis and a temporal feature on the vertical axis.<sup>8</sup> Figure 2 visualises the feature space with a clustering algorithm. Clustering is a

popular strategy to determine dividing lines by bringing together dots with similar features into clusters and nearest neighbours in the feature space. Here, data points are collected together depending on their between-ness measures by the distance from a central dot in each grouping (represented as black dots in Figure 2). Each algorithm divides the feature space within three spatially separate groups of data points, which could be spatio-temporal aggregates of particular predictions. While these figures visualise how two particular algorithms develop different decision boundaries based on two spatio-temporal features, all algorithms partition an abstract feature space based on the axialisation of a number of features. They all lead to partitions that organise the data points differently. Other commonly used algorithms in predictive analytics such as logistic regression or neural networks (Abbott 2014) that can learn more complex boundaries between subspaces of similar features also partition the feature space by drawing decision boundaries.

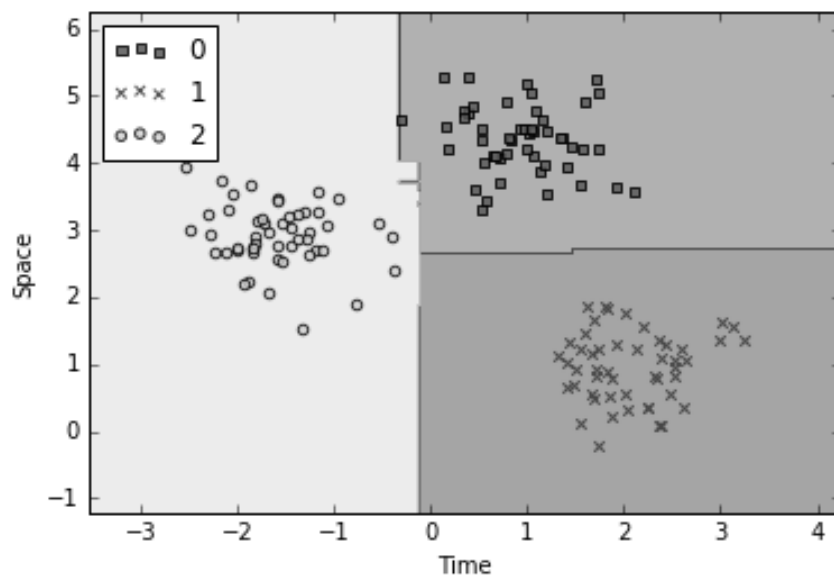


Figure 1, Decision tree algorithm

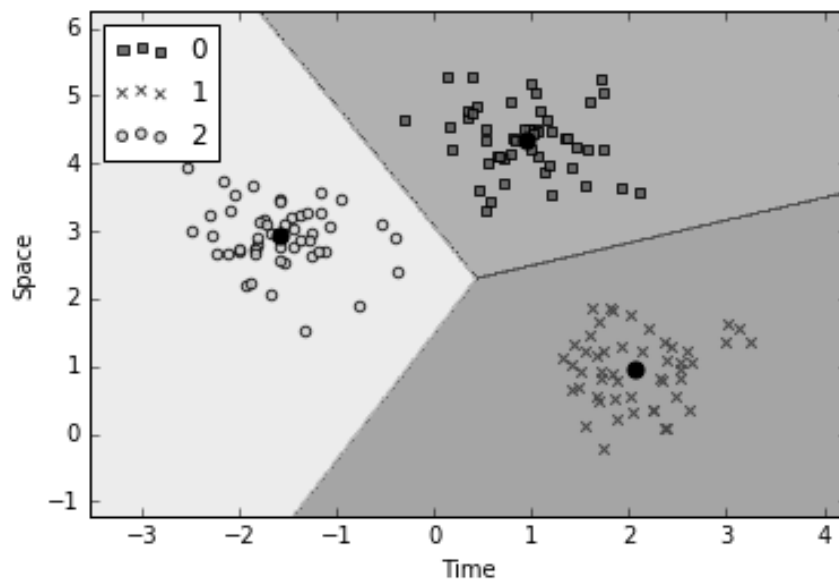


Figure 2, Clustering algorithm

What digital mode of prediction emerges through calculations of between-ness in the feature space? In the calculation of 'between-ness' as the shortest path between two data points, prediction is no longer harnessed to futurity either as a projection of the present norm or a prospective retro-diction of actuarial patterns. Chronological time and spatial coordinates are featurised to become calculable in the feature space. In that sense, the feature space can be understood as akin to what Deleuze called 'any-space-whatever' as 'a space of virtual conjunction, grasped as pure locus of the possible', where 'linkages can be made in an infinite number of ways' (1997, 109).

If between-ness actualises a limited number of the infinitely possible linkages that have measurable distances, it is not surprising that the language of predicting the future has been supplemented by the art of the predicting the present (Choi and Varian 2012) or even the 'past' (Schutt and O'Neil 2013). Google's chief economist, Hal Varian, contends that queries that users enter into Google's search engine describe how they feel and act in 'real time' (Choi and Varian 2012). Alongside predicting the future and the present, a third injunction to 'predict the past' with big data implies the counter-intuitive prediction of past performance by joining historical data sets. This way, security analysts have, for instance, identified historical spatio-temporal patterns of IED usage by the Provisional Irish Republican Army during 'The Troubles' and analysed the 'historical behaviour of terrorism' (Tench, Fry, and Gill 2016). In the case of policing, predictive analytics offers the promise of not just anticipating future crimes, but 'leading to more precise attribution of past crimes, and the apprehension of suspects' (Wang, Rudin, Wagner, and Sevieri 2013, 515).

In the feature space, between-ness can be about forward, backward or sideways connections. It captures the 'accidental or nonchronological relations' that appear to be 'better predictors of the future' (Chun 2016, 56). The relation between past, present and future has become indefinite, as predictive analytics forms models from any data to 'predict' relations between data points in particular situations. On the one hand, between-ness as the geometrical calculation of distance produces time as relation between data points. On the other, chronological, linear time is featurised in the abstract feature space in order to produce an eventual time of near-real-time decision-making. Predictive analytics is harnessed to the event of decision (rather than, say, the event of crime or of a terrorist attack) understood as quasi-synchronicity or quasi-simultaneity.

The reading of prediction developed here shows that time and space morph into each other through performative calculations of between-ness. Chronological time is spatialised in the feature space, while calculations of geometrical distances become temporalised as near-real-time decisions. The next section explores this actualisation of between-ness in security governance by addressing the time/space of predictive policing. It is perhaps in this morphing of time into space and space into time that big data most transgresses statistical techniques. It is in this continual variation and switch between time and space that predictive analytics and big data have most transformed security governance.

## Security in regime of ‘between-ness’: predictive policing

The predictive promise of big data has received a lot of public attention in the context of policing, with predictive policing one of the most recent articulations of a ‘big data revolution’ for security practices. Predictive policing takes its inspiration from other big data organisations and incorporates ‘more variables as some departments already have done, and perhaps even other data sources beyond police and government records like social media and news articles’ (CTOlabs 2013, 5). To unpack the actualisation of ‘between-ness’ in security governance we briefly discuss two tools used in predictive policing: Predpol, the software developed in collaboration with US police forces and increasingly integrated within policing practices in the US and UK, and predictive mapping software developed by scientists at University College London in collaboration with the Met Police in the UK, which promises to advance on the time/space featurisation of PredPol.

The new predictive policing tools rely on criminological theories about repeat and near-repeat crime in combination with the increased computational techniques of predictive analytics. PredPol, a predictive policing software initially developed by the anthropologist Jeffrey Brantingham at UCLA and the mathematician George Mohler at Santa Clara University in California, has exploited this combination of near-repeat theories with predictive analytics to become one of the most popular (and equally controversial) technologies, deployed by police forces across three continents.<sup>9</sup> For PredPol time/space considerations dominate its approach as it processes crimes by a combination of three features: what, when and where or type, time and location of crime (PredPol 2015a). Predictive policing software thus relies on the features of time and space that are recorded for crimes by the police and criminological assumptions about crime/event relatedness.

According to criminological assumptions that underpin PredPol, types of crimes are not ‘uniformly distributed within space and time’ (Short et al. 2008, 1249) and work ‘in a mathematical way, whether they [criminals] know it or not’ (Modesto Police Chief Galen Carroll quoted in PredPol 2015b). Translated in computing vocabularies, ‘crime tends to form dense clusters in space and time’ (Short, Bertozzi, and Brantingham 2010, 463) so that different clustering algorithms can be deployed to analyse the data. This ‘near-repeat risk’ of crime can be used to cluster dots in the abstract feature space (Mohler et al. 2012, 102). Predictive policing more generally promises to ‘surface particular times and locations predicted to be associated with an increased likelihood for crime’ (Beck and McCue 2009). In the UK, UCL scientists reiterate these spatio-temporal assumptions as they argue that predictive policing tools reflect ‘the strong spatial and temporal integration’ of all aspects of crime (Cheng et al. 2016, 6-7).

Spatio-temporal integration is not new to policing, as neighbourhoods, wards, beats and hotspots have long underpinned police and military action. The increased availability and collection of data, however, allows the proponents of predictive policing to articulate new governmental interventions that depart from traditional

statistically-based hotspot policing, which produced maps based on historical data of crime frequency. For Colleen McCue (2015, 24), policing needs to ‘shift from describing the past – counting, reporting, and “chasing” crime – to anticipation and influence in support of prevention, thwarting, mitigation, response, and informed consequence management’. Data-driven predictive policing technologies promise to be proactive rather than reactive, as historical data was thought to replicate the past rather than ‘intervening in emerging or future patterns of crime’ (CTOlabs 2013). In order to anticipate and predict, policing aims to deploy the latest mathematical and computing technologies to analyse spatio-temporal features of crime that deliver stable decision boundaries between the dots in the feature space.

As we have started discussing in the previous section, despite the future-oriented language in the advertisement and marketing of predictive policing tools, predictive politics through big data is not primarily about the turn to the future but about near-real-time decision-making. PredPol re-partitions its feature space daily in order to develop new spatio-temporal ‘between-ness’. As one of the co-founders of PredPol puts it, ‘Predictive policing in contrast consists of ranking hotspots on a daily basis according to estimated risk using both recent and historical crime incident data, rather than selecting a fixed set of hotspots for a several month intervention period’ (Mohler 2014). PredPol adjusts data processing to the time of police shifts so that it produces quasi-synchronicity rather than future-oriented prediction.

The near-real-time of predictive policing emerges through the calculation of ‘between-ness’ in the feature space. The spatialisation of crime events (largely violent crime) in the feature space produces daily updatable hotspots of crime. What counts for predictive policing is the production of ‘between-ness’ based on assumptions about spatio-temporal density of crime. Both PredPol and UCL predictive mapping use co-called ‘kernel clustering’ algorithms to distribute data points into a spatio-temporal ‘risk surface’ by summing contributions from nearby previous crimes, weighted according to how recently they occurred’ (Cheng et al. 2016, 8-9). Every day, PredPol produces a map of ‘500 square foot ‘hotspots’ where there is a higher probability of crime taking place relative to other local areas over the next 12 hours’ (Houses of Parliament 2015, 3). These spatio-temporal aggregates do not have to be real neighbourhoods, as they are abstract combinations of features. Hotspots are ‘spatio-temporal aggregates of criminal occurrences’ and ‘depend upon the particular geographic, economic, or seasonal conditions present’ (Short et al. 2008, 1249). Hotspots can be identified because there is less distance in-between particular combinations in the feature space. As abstract locations optimised to represent ‘between-ness’ in the feature space, hotspots are then overlaid on Google maps to produce ‘real’ hotspots to be policed.

PredPol calculates what we call ‘between-ness’ by clustering data points according to the spatio-temporal configuration of an earthquake which ‘increases the likelihood of another earthquake nearby in space and time’ (Mohler et al. 2012, 100). While the earthquake model marketed by PredPol has led to a lot of public and academic controversy, less attention has been paid to the production of feature spaces in these algorithms. Predictive policing models share an interest in crime regularities

in space and time that can be used to cluster dots in the feature space and make crimes predictable. The UCL's model promises to improve PredPol's mainly by a new network-based featurisation of time/space. According to these models, crimes induce a new high likelihood of a new crime happening in a similar time/space configuration. Research into predictive policing is thus focused on how to featurise this spatio-temporal regularity in order to produce smaller hotspots and near-real-time decision-making. The UCL scientists use street maps rather than regions or grids and thus claim that a more detailed featurisation of space is more appropriate (Cheng et al. 2016, 8-9).

Understood as a reconfiguration of time/space, predictive policing is not only a tool for governing 'others' but also for governing 'the self', as police resources have diminished in a neoliberal age (see Cheng et al. 2016, Mohler 2014). Or as a RAND evaluation of predictive policing puts it, 'predictive policing is not fundamentally about making crime-related predictions. It is about implementing business processes' (Perry 2013, 161). Hotspots reconfigure space away from the enclosed, artificially created space of the prison, the clinic or the asylum and the natural milieu influencing the life of populations. They emerge through featurised between-ness that relies on assumptions about geometrical distances based on criminological theories of spatio-temporal density of crime. Governmental techniques do not manipulate the 'givens' of a milieu through action at a distance, but intervene on indefinitely changing 'hotspots' (Cheng et al. 2016, 4-5).

Hotspots are between-ness actualised in near-real-time. A governmental apparatus of big data enacts prediction as between-ness calculations of similarity and difference. Between-ness is distinct from the 'docile bodies' of discipline or the population of biopolitical government, as it is the production of pure relationality, of geometrical connection as simultaneously similarity and difference. By featurising space, time and type of crime, PredPol experts can also argue that they use 'no personal information about individuals or groups of individuals, eliminating any personal liberties and profiling concerns' (PredPol 2015a). Yet, time/space configurations are not separate from the 'conduct of conduct' of subjects of government. What counts for a critical analysis of security and predictive policing is to develop vocabularies that challenge the regime of between-ness underpinning predictive policing with big data. Calculation of between-ness for predictive policing relies on time/space relationality to produce similarity and difference in the feature space. The most striking transformation of big data for security is how the reversibility of time and space through between-ness is translated into reversibility of similarity and difference. Similarity and difference are no longer opposed, but morph into each other. Security enactments of friend versus enemy, normal versus abnormal are now transformed through a modulated reversibility of time/space, similarity/difference that elude the structural categories of discrimination and exclusion deployed in critical thought on security.

## **Conclusion**

The emergence of big data has promised to transform digital capabilities and to revitalise predictive techniques for the purposes of security governance. This paper has argued that prediction has not vanished from governmental apparatuses, but that a digital mode of prediction has emerged as distinct from discipline's projection of the present 'norm' and biopolitical prospective normalisation based through a statistical calculation of frequencies. If prediction is understood as entwined with governmental apparatuses that shape the conduct of individuals and multiplicities, then it is also about time/space interventions rather than about taming the future. Although varied forms of data and algorithms are used for the purposes of prediction, we have shown that analytics with big data promises to use all kinds of data and thus needs to rely on calculations of between-ness in feature spaces, which are shared among different algorithms and digital analytics methods. We can thus speak of a regime of between-ness that calculates connections as the 'shortest path' between data points. Our illustration of predictive policing has shown how this between-ness is actualised as dynamic hotspots of near-real-time decision-making. In a regime of between-ness, time/space and similarity/difference morph into each other so that distinctions that security practices enact have become blurred.

The analysis developed here has three sets of implications for social and political theories of prediction and security in the age of big data. Firstly, our notion of between-ness attends to the specificities of digital practices and particularly the emergence of big data that go beyond discussions of network society or connexionist worlds (Savage 2013 see also the Introduction to the special issue). Predictive analytics enacts particular calculations of relationality as the 'shortest path' depending on feature combinations and decision boundaries. While algorithms remain secret, we need to attend more closely to the geometries that are implicated in these calculations and assumptions about time/space that undergird these geometries.

Secondly, security needs to be analysed as predictively enacted in artificial feature spaces rather than starting from a new future-orientation of governmental practices. Thus, critical analyses security practices – and of governmental apparatuses of big data more generally – which address the production of feature spaces need to unpack how a regime of between-ness produces continual reversibility of time/space and similarity/difference. Rather than focusing on the secrecy of algorithms, which is often compounded by the secrecy associated with security professionals, we can attend to how time and space, similarity and difference morph into each other. This also mean that critical vocabularies of discrimination and exclusion have become increasingly difficult to mobilise against security practices. Through the featurisation of time and space, PredPol has for example pre-emptively dis-activated accusations of discrimination. The reversibility and relationality produced in a regime of between-ness requires us to revisit relationality in social theory and develop critical vocabularies of relationality that grapple with big data governmentality.

Thirdly, the uses of prediction in security practices are currently harnessed not just to 'governing others', but to 'governing the self', understood here as organisations and security professionals in the neoliberal age. As public and private organisations collect more and more data, while other resources dwindle, predictive

analytics with big data needs to be understood as part of neoliberal economies mediating between abundance and scarcity. It is in that sense of mobilising economies of data abundance to address scarcity that we can also understand the attitude that many practitioners harbour towards error. While they aim to reduce error in data, they also acknowledge the indispensability of prediction with big data: ‘predicting better than pure guesswork, even if not accurately, delivers real value’ (Siegel 2013, 11). Thus, techniques of prediction are difficult to criticise on the basis of failure or inefficiency, as evaluations of predictive policing by civil rights organisations and critical scholars have pointed out (e.g. Statewatch 2014). The neoliberal economies of big data abundance and excess efface the modes of scarcity, lack of resources and privatisation constitutive of big data governmentality today.

## Notes

---

<sup>1</sup> Although prediction is not equivalent to anticipation, regimes of anticipation rely on prediction and simulation (Mackenzie 2013, 392). We focus on prediction, as the language and methods of predictive analytics inform the security practices we analyse here.

<sup>2</sup> Discipline as an analytics of space has been widely invoked in readings of Foucault’s in geography (e.g. Crampton and Elden 2007).

<sup>3</sup> Surveillance studies scholars have increasingly challenged the model of the Panopticon, whose focus on architecture does not capture recent surveillance practice (Haggerty 2006) and have addressed the conjunction of space and time in surveillance (Lyon 2006).

<sup>4</sup> It is only recently that Foucault’s concept of the milieu has started to receive analytical attention (Ansems de Vries 2014, O’Grady 2013).

<sup>5</sup> We follow here the distinction by Eric Siegel between machine learning and predictive analytics, where he sees the latter as the language of practitioners. The boundaries of machine learning and predictive analytics are, however, fuzzy.

<sup>6</sup> Our selection of practitioners’ book focuses on the books that most appear on blogs and are recommended by the Predictive Analytics World conference: Eric Siegel, Dean Abbott, Thomas Davenport, Foster Provost. Abbott’s blog is one of the top ten online reference sources for predictive analytics (<http://abbottanalytics.blogspot.co.uk/>). Colleen McCue’s work has been mediatized and widely use in applications of predictive analytics to security and policing. Finally, we use two predictive policing tools developed through collaboration between academics and police to analyse the details of predictive analytics in its most successful contemporary use case. Given the academic participation, details about the features used and data are available in published literature.

<sup>7</sup> Our methodological experiment was also made possible through our interdisciplinary backgrounds in security studies and social informatics. While the discussion of our interdisciplinary collaboration is beyond the scope of this paper, we acknowledge that interdisciplinary collaboration is not devoid of agonism (see Barry, Born, and Wesszkalnys 2008).

<sup>8</sup> For the example, we have generated a random data set of 150 observations distributed in space and time that are distributed over three distinct regions, the algorithms need to divide.

<sup>9</sup> In 2016, PredPol was entered into the GovTech 100, the top 100 list of companies focused on technology for the public sector (Government Technology 2016).



---

## References

- Abbott, D (2014) *Applied Predictive Analytics: Principles and Techniques for the Professional Data Analyst*. London: John Wiley & Sons.
- Adam, B, and C Groves (2007) *Future Matters: Action, Knowledge, Ethics*. Leiden: Brill.
- Adams, V, M Murphy, and AE Clarke (2009) Anticipation: Technoscience, life, affect, temporality. *Subjectivity* vol. 28 (1):246-265.
- Adey, P (2009) Facing airport security: affect, biopolitics, and the preemptive securitisation of the mobile body. *Environment and Planning D: Society and Space* vol. 27 (2):274-295.
- Akhgar, B, et al. (2015) *Application of Big Data for National Security. A Practitioner's Guide to Emerging Technologies*. Amsterdam: Butterworth-Heinemann.
- Amoore, L (2011) Data derivatives. *Theory, Culture & Society* vol. 28 (6):24-43. doi: 10.1177/0263276411417430.
- Amoore, L (2014) *The Politics of Possibility: Risk and security beyond probability*. Durham, NC: Duke University Press.
- Ansems de Vries, L (2014) *Re-imagining a Politics of Life: From Governance of Order to Politics of Movement*. London: Rowman & Littlefield International.
- Aradau, C (2015) The signature of security: Big data, anticipation, surveillance. *Radical Philosophy* (191):21-28.
- Aradau, C, and T Blanke (2015) The (Big) Data-security assemblage: Knowledge and critique. *Big Data & Society* vol. 2 (2):1-12. doi: 10.1177/2053951715609066.
- Aradau, C, and R van Munster (2011) *Politics of Catastrophe: Genealogies of the unknown*. Abingdon: Routledge.
- Barry, A, G Born, and G Wieszkalnys (2008) Logics of interdisciplinarity. *Economy and Society* vol. 37 (1):20-49.
- Beck, C, and C McCue (2009) Predictive policing: what can we learn from Wal-Mart and Amazon about fighting crime in a recession? *Police Chief* 76 (November), [http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article\\_id=1942&issue\\_id=112009](http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1942&issue_id=112009).
- Beck, U (2009) *World at Risk*. Cambridge: Polity.
- Bigo, D (2008) Security: A Field Left Fallow. In *Foucault on Security and War*, edited by Michael Dillon and Andrew Neal, 93-114. Basingstoke: Palgrave Macmillan.
- boyd, d, and K Crawford (2012) Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society* vol. 15 (5):662-679.

- 
- Chan, J, and L Bennett Moses (2015) Is Big Data challenging criminology?  
*Theoretical Criminology*:1362480615586614. doi:  
10.1177/1362480615586614.
- Cheng, T, et al. (2016) CPC: Crime, Policing and Citizenship – Intelligent policing  
and big data. London: UCL SpaceTime Lab.
- Choi, H, and H Varian (2012) Predicting the present with google trends.  
*Economic Record* vol. 88 (s1):2-9.
- Chun, WHK (2016) *Updating to Remain the Same: Habitual New Media*.  
Cambridge, Mass.: MIT Press.
- Crampton, JW (2015) Collect it all: national security, Big Data and governance.  
*GeoJournal* vol. 80 (4):519-531. doi: 10.1007/s10708-014-9598-y.
- Crampton, JW, and S Elden (2007) *Space, knowledge and power: Foucault and  
geography*: Ashgate Publishing, Ltd.
- CTOlabs (2013) *To Protect and Serve with Big Data* 2013 [cited 27 December  
2015].
- Cukier, K, and V Mayer-Schoenberger (2013) Rise of Big Data: How it's Changing  
the Way We Think about the World, The. *Foreign Affairs* vol. 83.
- Davenport, T (2014a) *Big Data at Work: Dispelling the Myths, Uncovering the  
Opportunities*. Boston, Mass.: Harvard Business Review Press.
- Davenport, T (2014b) Preface. In *Predictive Analytics, Data Mining and Big Data:  
Myths, Misconceptions and Methods*, edited by Steven Finlay. Basingstoke:  
Palgrave.
- Dean, M (1999) *Governmentality. Power and Rule in Modern Society*. London:  
Sage.
- Deleuze, G (1997) *Cinema 1. The Movement-Image*. Minneapolis: University of  
Minnesota Press.
- Dhar, V (2013) Data science and prediction. *Communications of the ACM* vol. 56  
(12):64-73.
- Dillon, M (2007) Governing through contingency: The security of biopolitical  
governance. *Political Geography* vol. 26 (1):41-47.
- Ekbja, H, et al. (2015) Big data, bigger dilemmas: A critical review. *Journal of the  
Association for Information Science and Technology* vol. 66 (8):1523-1545.  
doi: 10.1002/asi.23294.
- Ewald, F (2011) Omnes et singulatim. After risk. *The Carceral* vol. 7:77-107.
- Ewald, F (2012) *Assurance, prévention, prédiction ...dans l'univers du Big Data*.  
Institut Montparnasse 2012 [cited 31 July 2015]. Available from  
[http://www.institut-montparnasse.fr/wp-  
content/files/Collection\\_recherches\\_n\\_4.pdf](http://www.institut-montparnasse.fr/wp-content/files/Collection_recherches_n_4.pdf).
- Foucault, M (1978) *The History of Sexuality. Volume I*. New York: Pantheon Books.
- Foucault, M (1986) Of other spaces. *diacritics* vol. 16 (1):22-27.
- Foucault, M (2007) *Security, Territory, Population*. Basingstoke: Palgrave.

- 
- Foucault, M (2008) *Psychiatric power: Lectures at the college de france, 1973-1974*. New York: Palgrave Macmillan.
- GCHQ (2011) 'ICTR Cloud Efforts'. *Developing 'canonical' SIGINT analysis, finding hard targets and exploratory data analysis at scale* 2011 [cited 30 March 2016]. Available from <https://search.edwardsnowden.com/docs/ICTRCloudEffects2015-09-25nsadocs>.
- Gordon, C (1991) Governmental rationality: An introduction. In *The Foucault Effect: Studies in Governmentality*, edited by Graham Burchell, Colin Gordon and Peter Miller, 1-51. Hemel Hempstead: Harvester Wheatsheaf.
- Government Technology (2016) *Next Wave of Civil Innovation* 2016 [cited 15 February 2016]. Available from <http://www.govtech.com/100/>.
- Hacking, I (1982) Biopower and the avalanche of printed numbers. *Humanities in Society* vol. 5:279-295.
- Haggerty, KD (2006) Tear down the walls: on demolishing the panopticon. In *Theorizing surveillance: The panopticon and beyond*, edited by David Lyon, 23-45. London: Routledge.
- Hansen, HK (2015) Numerical operations, transparency illusions and the datafication of governance. *European Journal of Social Theory* vol. 18 (2):203-220. doi: 10.1177/1368431014555260.
- Harcourt, BE (2008) *Against prediction: Profiling, policing, and punishing in an actuarial age*. Chicago: University of Chicago Press.
- Houses of Parliament (2015) Big Data, crime and security. *Postnote*, <http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-470-fullreport>.
- Introna, LD (2015) Algorithms, Governance, and Governmentality: On Governing Academic Writing. *Science, Technology & Human Values*. doi: 10.1177/0162243915587360.
- Janert, PK (2010) *Data analysis with open source tools*. Cambridge, MA: O'Reilly Media.
- Kitchin, R (2014) *The data revolution: Big data, open data, data infrastructures and their consequences*. London: Sage.
- Koselleck, R (2004) *Futures Past. On the Semantics of Historical Time*. Translated by Keith Tribe. New York: Columbia University Press.
- Lakoff, A (2007) Preparing for the next emergency. *Public Culture* vol. 19 (2):247.
- Lohr, S (2015) *Data-ism: The Revolution Transforming Decision Making, Consumer Behavior, and Almost Everything Else*. Harper Collins.
- Lyon, D (2006) *Theorizing surveillance*. London: Routledge.
- Lyon, D (2014) Surveillance, Snowden, and big data: capacities, consequences, critique. *Big Data & Society* vol. 1 (2):2053951714541861.

- 
- Mackenzie, A (2015) The production of prediction: What does machine learning want? *European Journal of Cultural Studies* vol. 18 (4-5):429-445. doi: 10.1177/1367549415577384.
- Massumi, B (2009) National enterprise emergency steps toward an ecology of powers. *Theory, Culture & Society* vol. 26 (6):153-185.
- McCue, C (2015) *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. 2nd edition ed. Oxford: Butterworth-Heinemann.
- Meier, P (2015) *Digital humanitarians: how big data is changing the face of humanitarian response*. Boca Raton: CRC Press.
- Minois, G (1996) *Histoire de l'avenir*. Paris: Fayard.
- Mohler, G (2014) Marked point process hotspot maps for homicide and gun crime prediction in Chicago. *International Journal of Forecasting* vol. 30 (3):491-497.
- Mohler, GO, et al. (2012) Self-exciting point process modeling of crime. *Journal of the American Statistical Association* vol. 106 (493):100-108.
- National Security Agency (2008) *Boundless Informant. Frequently Asked Questions* 2008 [cited 30 March 2016]. Available from <https://search.edwardsnowden.com/docs/BoundlessInformant%E2%80%9093FrequentlyAskedQuestions2013-06-08nsadocs>.
- O'Grady, N (2013) Adopting the position of error: space and speculation in the exploratory significance of milieu formulations. *Environment and Planning D: Society and Space* vol. 31 (2):245-258.
- O'Malley, P (2004) *Risk, Uncertainty and Government*. London: The GlassHouse Press.
- Pasquale, F (2015) *The Black Box Society*. Cambridge, MA: Harvard University Press.
- Perry, WL (2013) *Predictive policing: The role of crime forecasting in law enforcement operations*: RAND Corporation.
- PredPol (2015a) *Scientifically proven field results*. PredPol 2015a [cited 10 October 2015]. Available from <http://www.predpol.com/results/>.
- PredPol (2015b) *Technology* 2015b [cited 10 October 2015]. Available from <http://www.predpol.com/technology/>.
- Provost, F, and T Fawcett (2013) *Data Science for Business: What you need to know about data mining and data-analytic thinking*. Sebastopol, CA: O'Reilly Media.
- Rouvroy, A (2010) Gouverner: Détecter et prévenir! *Politique* vol. 61:14-17.
- Samimian-Darash, L, and P Rabinow (2015) *Modes of Uncertainty: Anthropological Cases*. Chicago: University of Chicago Press.
- Savage, M (2013) Digital fields, networks and capital: Sociology beyond structures and fluids. In *Digital Sociology: Critical Perspectives*, edited by Kate Orton-Johnson and Nick Prior, 139-150. Basingstoke: Palgrave.

- 
- Schutt, R, and C O'Neil (2013) *Doing data science: Straight talk from the frontline*: O'Reilly Media, Inc.
- Short, MB, AL Bertozzi, and PJ Brantingham (2010) Nonlinear patterns in urban crime: Hotspots, bifurcations, and suppression. *SIAM Journal on Applied Dynamical Systems* vol. 9 (2):462-483.
- Short, MB, et al. (2008) A statistical model of criminal behavior. *Mathematical Models and Methods in Applied Sciences* vol. 18 (supp01):1249-1267. doi: doi:10.1142/S0218202508003029.
- Siegel, E (2013) *Predictive analytics: The power to predict who will click, buy, lie, or die*. Hoboken, NJ: John Wiley & Sons.
- Statewatch (2014) *Note on big data, crime and security: Civil liberties, data protection and privacy concerns* (3 April 2014). Statewatch 2014 [cited 29 August 2015]. Available from <http://www.statewatch.org/analyses/no-242-big-data.pdf>.
- Tench, S, H Fry, and P Gill (2016) Spatio-temporal patterns of IED usage by the Provisional Irish Republican Army. *European Journal of Applied Mathematics* vol. 27 (Special Issue 03):377-402. doi: doi:10.1017/S0956792515000686.
- Van Rijsbergen, K (2004) *The geometry of information retrieval*. Cambridge University Press Cambridge.
- Wang, T, C Rudin, D Wagner, and R Sevieri (2013) Learning to Detect Patterns of Crime. In *Machine Learning and Knowledge Discovery in Databases*, edited by Hendrik Blockeel, Kristian Kersting, Siegfried Nijssen and Filip Železný, 515-530. Springer Berlin Heidelberg.
- Wood, DM (2007) Beyond the Panopticon? Foucault and surveillance studies. In *Space, knowledge and power: Foucault and geography*, edited by Jeremy W Crampton and Stuart Elden, 245-263. Hampshire: Ashgate.